In the Claims:

Please amend Claims 57, and add new Claims 96-99, all as shown below. Applicant respectfully reserves the right to prosecute any originally presented or canceled claims in a continuing or future application. This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

1-56. (Canceled)

57. (Currently Amended) A system for maintaining security in a distributed computing environment, comprising:

a policy manager located on a server [[for]] to:

~~creating~~ a local security policy derived from a global security policy, said global security policy including a plurality of rules applicable to all application guards in the system, wherein creating the local security policy includes determining which of the plurality of rules of the global security policy are applicable to a particular application guard such that the local security policy contains a fewer number of rules than said global security policy; and ~~for~~

~~distributing~~ the local security policy to said client wherein the local security policy includes the rules customized to the application guard, said rules including a set of grant rules that allow access to securable components and a set of deny rules that prevent access to said securable components; and

an application guard located at the client [[for]] to manage ~~managing~~ access by individual transactions to securable components at a client level as specified by the local security policy, the securable components including at least one application wherein said application guard is integrated into said application and controls access to the application with which the application guard is integrated;

wherein the application guard receives an authorization request including a subject, an object and a privilege and evaluates said request by matching the rules received from the policy manager to said subject, said object and said privilege in order to control access to said application integrated with the application guard.

58. (Previously presented) The system of Claim 57 wherein said securable components further include a function within the application as specified by the security policy.

59. (Withdrawn) The system of Claim 57 including a procedure within the application as specified by the security policy.

60. (Withdrawn) The system of Claim 57 including a data structure within the application as specified by the security policy.

61. (Withdrawn) The system of Claim 57 including a database object referenced by the application as specified by the security policy.

62. (Withdrawn) The system of Claim 57 including a file system object referenced by the application as specified by the security policy.

63. (Previously presented) A method for maintaining security in a distributed computing environment, comprising:

receiving a global security policy that includes a plurality of rules for regulating access to securable components in the system, the securable components including at least one application wherein said rules of the global security policy apply to all application guards in the distributed computing environment;

creating a local security policy via a policy manager located on a server, the local security policy including a plurality of rules customized to a client wherein creating the local security policy includes customizing the local security policy by determining which of the rules from the global security policy are applicable to a specific application guard located on the client such that the local security policy contains a fewer number of rules than said global security policy;

distributing the local security policy to the client; and

receiving an authorization request by the application guard, the authorization request including a subject, an object and a privilege wherein said application guard is integrated into said application and controls access to the application with which the application guard is integrated;

managing access as specified by the local security policy via the application guard located at the client to securable components wherein managing access includes comparing the subject, object and privilege to the rules of the local security policy.

64. (Withdrawn) The method of Claim 63 wherein the securable components include a function within the application as specified by the security policy.

65. (Withdrawn) The method of Claim 63 including a procedure within the application as specified by the security policy.

66. (Withdrawn) The method of Claim 63 including a data structure within the application as specified by the security policy.

67. (Withdrawn) The method of Claim 63 including a database object referenced by the application as specified by the security policy.

68. (Withdrawn) The method of Claim 63 including a file system object referenced by the application as specified by the security policy.

69-71. (Canceled).

72. (Previously presented) A method for maintaining security in a distributed computing environment, comprising the steps of:

receiving a global security policy that includes a plurality of rules for regulating access to securable components in the system, the securable components including at least one application wherein said rules of the global security policy apply to all application guards in the distributed computing environment;

providing a policy manager located on a server to create a local security policy including a plurality of rules customized to a client wherein creating the local security policy includes customizing the local security policy by determining which of the rules from the global security policy are applicable to a specific application guard located on the client such that the local security policy contains a fewer number of rules than said global security policy;

distributing the local security policy to the client;

providing an application guard located at the client to manage access to securable components at a client level as specified by the local security policy, said application guard being integrated into said application and controlling access to the application with which the application guard is integrated;

receiving an authorization request by the application guard, said authorization request including a subject, an object and a privilege; and

controlling access to the securable components by matching the subject, object and privilege to the rules of the local security policy by the application guard.

73. (Previously presented) The method of Claim 72 wherein the securable components include a function within the application as specified by the security policy.

74. (Withdrawn) The method of Claim 72 including a procedure within the application as specified by the security policy.

75. (Withdrawn) The method of Claim 72 including a data structure within the application as specified by the security policy.

76. (Withdrawn) The method of Claim 72 including a database object referenced by the application as specified by the security policy.

77. (Withdrawn) The method of Claim 72 including a file system object referenced by the application as specified by the security policy.

78-80. (Canceled).

81. (Previously presented) A computer readable storage medium having stored thereon a set of instructions to execute a method for maintaining security in a distributed computing environment comprising the steps of:

receiving a global security policy that includes a plurality of rules for regulating access to securable components in the system, the securable components including at least one

application wherein said rules of the global security policy apply to all application guards in the distributed computing environment;

creating a local security policy via a policy manager located on a server, the local security policy including a plurality of rules customized to a client wherein creating the local security policy includes customizing the local security policy by determining which of the rules from the global security policy are applicable to an application guard located on the client such that the local security policy contains a fewer number of rules than said global security policy;

distributing the local security policy to the client; and

receiving an access request by the application guard, said access request including a subject, an object and a privilege wherein said application guard is integrated into said application and controls access to the application with which the application guard is integrated;

matching the access request to at least one rule selected from the rules of the local security policy in order to manage access as specified by the local security policy via the application guard located at the client to securable components.

82. (Withdrawn) The computer readable storage medium of Claim 81 wherein the securable components include a function within the application as specified by the security policy.

83. (Withdrawn) The computer readable storage medium of Claim 81 including a procedure within the application as specified by the security policy.

84. (Withdrawn) The computer readable storage medium of Claim 81including a data structure within the application as specified by the security policy.

85. (Withdrawn) The computer readable storage medium of Claim 81 including a database object referenced by the application as specified by the security policy.

86. (Withdrawn) The computer readable storage medium of Claim 81 including a file system object referenced by the application as specified by the security policy.

87-89. (Canceled).

90. (Previously Presented) The system of claim 57, wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.

91. (Previously presented) The system of claim 90, wherein the global policy specifies access privileges of a user to securable components.

92. (Previously presented) The method of claim 72, wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.

93. (Previously presented) The method of claim 92, wherein the global policy specifies access privileges of a user to securable components.

94. (Previously presented) The computer readable storage medium of claim 81, wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.

95. (Previously presented) The computer readable storage medium of claim 94, wherein the global policy specifies access privileges of a user to securable components.

96. (New) The system of Claim 57 wherein said policy manager is further capable of optimizing said global security policy into an optimized form, wherein the optimized form only distributes attributes relevant to a specific application guard.

97. (New) The system of Claim 57 wherein said policy manager is further capable of:

receiving a modification on a existing security policy;

computing any differences caused by the modification on the security policy; and

committing only the changed portion of the security policy to an appropriate application guards.

98. (New) The system of Claim 57 wherein said application guard is further capable of being associated with plug-ins to allow for additional capabilities based on customized code.